UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,343	07/14/2001	Anjali Chandnani	655/62439	3770

7590 01/13/2005

Richard F. Jaworski
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/905,343	CHANDNANI ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-23 have been considered.

Claim Objections

Claim 23 is objected to because of the following informalities: the phrase "wherein detection engine" should be "wherein the detection engine". Appropriate correction is required.

Claim Rejections - 35 USC § 112

Claims 10 and 11 are rejected under U.S.C. 112, 4th paragraph. Claim 10 is a dependent claim which fails to further limit independent claim 1 on which it depends. It is well known in the art that lexical analysis is the process of taking an input string and producing a sequence of tokens. Since the data stream is lexically analyzed according to claim 1 part c, it is assumed that a series of tokens has been produced as a result. Claim 10 has therefore been withdrawn from consideration. Claim 11, which depends on claim 10, is withdrawn as well.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1,7-9,13-16, and 22-23 are rejected under 35 U.S.C. 102(a) as being anticipated by Fermoyle, (Fermoyle, Ken. Firm Offers Free Tool to Fight 'Love You' Virus. June 2000. Ottawa PC User's Group).

As per claims 1 and 13-16, the applicant describes a method of detecting a script language virus comprising the following limitations which are met by Fermoyle:

a) preparing language description data corresponding to at least one script language (paragraph 8);

b) preparing detection data for viral code corresponding to the script language virus (paragraph 8);

c) lexically analyzing a data stream using the language description data and the detection data to detect the viral code (paragraph 8);

In his newsletter, Fermoyle describes the malicious "I love you" virus. The "I love you" virus, as described by Edwards (Edwards, Mark Joseph. Love Letter Virus- An Update. May 5, 2000. Windows IT Pro) was a script virus which originated in the spring of 2000. In order to counter the script virus, as reported by Fermoyle, the product MailMarshal quarantined messages through the use of lexical scanning.

As discussed in the website literature online (www.essential.co.uk/Products/Mailmarshal/emailabuse_antivirus.asp), MailMarshal is a unique virus scanning system which seeks to solve the same problem identified in the applicant's disclosed invention: the problem that current "virus scanners will only detect existing viruses that they recognize by a signature" (page 1). As such, "MailMarshal's advantage lies in its ability to detect and block new viruses. MailMarshal can do this in a variety of ways: MailMarshal has a lexical text censor, so it can detect keywords or phrases in messages and attachments. Companies often know the names or key words associated with new viruses ('I love you', 'Life Stages', ...etc)" (page 2). The applicant should note that the examiner is aware that the MailMarshal literature was last updated in 2003, after the applicant's effective filing date. This is probably due to the fact that company websites are continually updated over the years. However, MailMarshal was known and used as a lexical scanner of viruses, in particular script viruses, before the applicant's effective filing date, as discussed by Fermoyle, Discussion of how MailMarshal works is only included to complement the user's understanding of the product, and the ideas

which will be used to form a 102a rejection will be taken from Fermoyle and other sources before the effective filing date.

Regarding part a), the language description data is particular keywords which correspond to viruses the MailMarshal counters. According to Fermoyle, the "'I love you' virus and its various mutations" (paragraph 1) are countered by MailMarshal. In other words, the system searches for a plurality of viruses. As described by Edwards, the "I love you" virus is a script virus. Furthermore, users or system administrators can effectively remove the threat of malicious viruses by "monitoring and controlling key words (lexical scanning)" (paragraph 8).

Regarding part b), the detection data is data which the scanner uses to determine how to search for the keywords within the file. After lexical analysis takes place, in other words, there must exist a mechanism in the scanner for telling it where and how to look for the keywords within the parsed data. This is the detection data.

Regarding part c), MailMarshal lexically scans the messages for the keywords (part a) through the use of data which helps it determine how to look for the keywords (part b).

Regarding claim 14, since the MailMarshal product is used on a computer, the additional limitation of a processor would be met by the computer system with the MailMarshal product running on it.

As per claim 7, the applicant limits the method of claim 1, which is met by Fermoyle (see above), with the following limitation which is also met by Fermoyle:

Further comprising setting language definition rules for each of the at least one script language (paragraph 8);

The MailMarshal uses language definition rules to search for particular keywords within the viruses.

As per claims 8,9, and 22, the applicant limits claims 1 and 16, which are met by Fermoyle (see above), with the following limitation which is also met by Fermoyle:

Wherein the detection data comprise at least one test, wherein each of the at least one test correspond to a pattern match or a cyclical redundancy check (paragraph 8);

The MailMarshal system uses pattern matching. MailMarshal monitors for particular keywords within a message. If the keywords "I love you" were searched for, for example, any identification of this pattern of words would cause the scanner to believe that the message is viral.

Regarding claim 9, part c) is met by the rejection above. Parts a) and b), in which samples of the viral code are obtained and analyzed, are met through the nature of the MailMarshal which obtains incoming messages (which are sometimes viral) and lexically analyzes them to determine whether or not they are in fact viral.

As per claim 23, the applicant limits the apparatus of claim 16, which is met by Fermoyle (see above), with the following limitation which is also met by Fermoyle.

Wherein detection engine converts the data stream to a stream of tokens using lexical analysis, and the tokens correspond to respective language constructs (paragraph 8);

As described earlier, the conversion of the data stream to a stream of tokens is implicit in the use of lexical analysis as described in part c) of claim 16. The fact that the tokens correspond to respective language constructs is met by the MailMarshal in the particular instance described because a script language virus (the "I love you" virus) is being lexically analyzed. The tokens would be language constructs of the script language virus.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-3 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fermoyle in view of Frame Technology.

As per claim 2-3 and 17-18, the applicant limits the method of claims 1 and 16, which are met by Fermoyle (see above), with the following limitation which is met by Frame Technology:

Wherein the language description data correspond to Dynamic Finite Automata;

As discussed by Frame Technology, one anti-viral technique is the use of finite automata which have states which vary and are dynamic. Since the states are dynamic, a set of transitions and next states is understood.

Claims 4-6 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fermoyle.

As per claims 4 and 19, the applicant limits the method of claims 1 and 16, which are met by Fermoyle (see above), with the following limitation which is also met by Fermoyle:

Wherein the language description data correspond to language definition rules and language check rules (paragraph 8);

As discussed above, the scanner uses language definition rules in the form of keywords or groups of keywords to determine whether a message is viral. However, the use of language check rules is not mentioned. As defined by the applicant, language check rules are characteristics of the target script languages which differentiate one language from another language (Specification page 8). Other than the obvious difference in that the keywords the scanner looks for are different, there is no mention of differentiation of rules for the different viruses. Since different viruses are searched for (paragraph 1), it would have been obvious to one of ordinary skill in the art at the time the invention was filed to have appropriate language check rules for the different languages.

As per claims 5 and 20, the applicant limits the method of claims 4 and 19, which are met by Fermoyle (see above), with the following limitation which is also met by Fermoyle:

Wherein the lexical analysis includes one or more pattern matches based on the language definition rules (paragraph 8);

The use of pattern matching is present in Fermoyle and discussed in the rejection for claim 8 and 22. However, claims 5 and 20 are rejected under U.S.C. 103(a) because they depend on claims 4 and 19.

As per claims 6 and 21, the applicant limits the method of claims 4 and 19, which are met by Fermoyle (see above), with the following limitation which is also met by Fermoyle:

Wherein a script language used by the data stream is determined by the lexical analysis using the language check rules;

The particular language used is determined through the monitoring of keywords. However, the particular language used is not determined through the language check rules because no language check rules are mentioned. Since different viruses are searched for (paragraph 1), it would have been obvious to one of ordinary skill in the art at the time the invention was filed to have appropriate language check rules for the different languages which allow the scanner to know which script language is being used.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fermoyle in view of the applicant's admitted prior art.

As per claim 12, the applicant describes the method of claim 10, which is met by Fermoyle (see above), with the following limitation which is met by the applicant's admitted prior art:

Wherein a cyclical redundancy check is performed on the stream of tokens to detect viral code;

As discussed by the applicant on page 3 of the Specification, one type of anti-virus technique is cyclical redundancy check. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas discussed by Fermoyle with those of the applicant's admitted

prior art and use a cyclical redundancy check on the stream of tokens for another way to detect viral code using the well-known CRC method on the stream of tokens created by the lexical scanning of the MailMarshal.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER